(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
11 March 2004 (11.03.2004)

PCT

(10) International Publication Number
WO 2004/021638 A1

(51) International Patent Classification[7]: H04L 9/00

(21) International Application Number: PCT/US2003/026834

(22) International Filing Date: 28 August 2003 (28.08.2003)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/406,721 28 August 2002 (28.08.2002) US
60/412,221 20 September 2002 (20.09.2002) US

(71) Applicant *(for all designated States except US)*: **DOCOMO COMMUNICATIONS LABORATORIES USA, INC.** [US/US]; 181 Metro Drive, Suite 300, San Jose, CA 95110 (US).

(72) Inventor; and
(75) Inventor/Applicant *(for US only)*: **GENTRY, Craig** [US/US]; 230 Houghton St., Mountain View, CA 94041 (US).

(74) Agent: **HORIE, Tadashi**; Brinks Hofer Gilson & Lione, P.O. Box 10087, Chicago, IL 60610 (US).

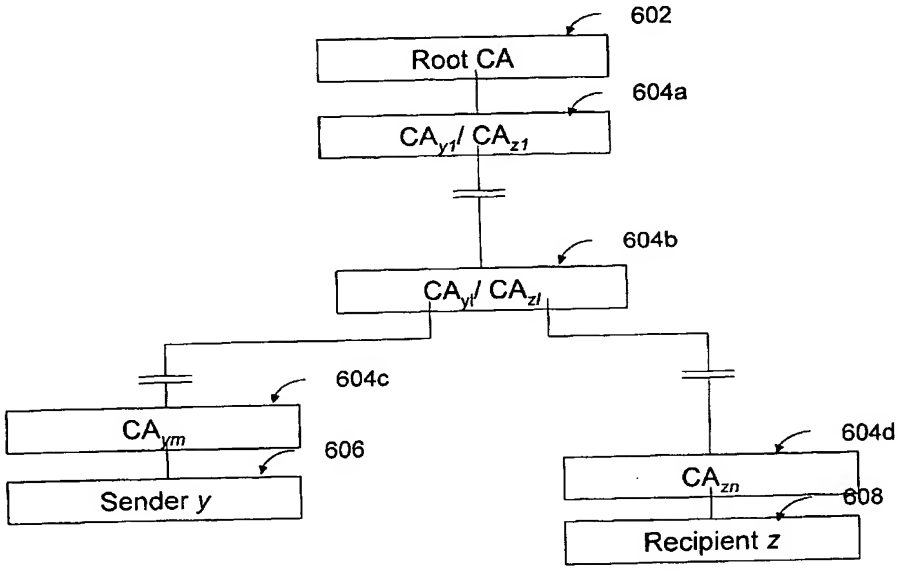
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*
— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

[Continued on next page]

(54) Title: CERTIFICATE-BASED ENCRYPTION AND PUBLIC KEY INFRASTRUCTURE



(57) Abstract: The present invention provides methods for sending a digital message from a sender (606) to a recipient (608) in a public-key based cryptosystem comprising an authorizer (606). The authorizer can be a single entity (606) or comprise a hierarchical or distributed entity (602, 604a-604b). The present invention allows communication of messages by an efficient protocol, not involving key status queries or key escrow, where a message recipient (608) can decrypt a message from a message sender (606) only if the recipient (608) possesses up-to-date authority from the authorizer. The invention allows such communication in a system comprising a large number (e.g. millions) of users.

WO 2004/021638 A1